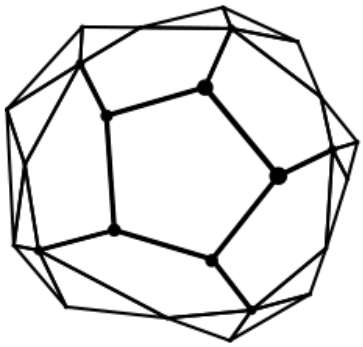

Nebula One User's Guide

Release 1.0.2

Nebula, Inc.

May 17, 2013

Notice

©2013, Nebula, Inc. All rights reserved.

CONTENTS

1 Nebula One User's Guide **1**

1.1 Access the Nebula One System and Request an Account . . . 1
1.2 Log In . . . 1
1.3 Create or Launch Instances . . . 2
1.4 Access an Instance from the Virtual Console . . . 3
1.5 Access an Instance Over the Network . . . 3
1.6 Terminate (Delete) an Instance . . . 4
1.7 Create an Instance Snapshot . . . 4
1.8 Launch an Instance from a Snapshot . . . 4
1.9 Delete an Instance Snapshot . . . 4
1.10 Manage Security Groups . . . 4
1.11 Manage Floating IP Addresses . . . 6
1.12 Manage Key Pairs . . . 7
1.13 Manage Volumes . . . 8
1.14 Manage Instances . . . 10
1.15 Advanced Interaction with CLIs and APIs . . . 10
1.16 Glossary . . . 10

CHAPTER

ONE

NEBULA ONE USER'S GUIDE

Nebula One consists of Nebula hardware and software coupled with certified industry-standard x86 servers known as Nebula Cloud Nodes to create a private cloud. Before you can use Nebula One, you must request an account from your system administrator.

1.1 Access the Nebula One System and Request an Account

In a web browser, navigate to the URL provided by your administrator for access to the Nebula One system.

1. On the login page, click *Request an Account*.
2. Complete the form with your preferred user name, existing email address, and preferred password and click *Send* to submit.

Your Nebula One administrator can now approve your request. Once your account has been approved by an administrator, you can log in.

1.2 Log In

1. In a web browser, navigate to the URL provided for access to the Nebula One system.
2. Log in using the username and password you requested for your account.

1.2.1 Use the Home Page

The Home Page shows all projects for which you are a member, and each project contains applications. A *project* is used to group users. By default, each user is a member of an automatically created project named `<username>-Home` for which they are the only member. Other projects can be created by administrators; these projects can have multiple members, all of whom share the same resources and quota.

The quick navigation menu located near the top left of the Home page lists the top-most project's name. Selecting another project in this menu will automatically scroll the browser to the selected project. A *application* enables access to key features of the Nebula One system. The applications shown for a particular project are based on your role within that project: administrator applications for administrators and user applications for users. Because you might have the same role in several projects, some applications might be repeated. Each of these applications, however, provides access only to its project's resources. To work within a project, simply open a application belonging to that project.

As a user, the primary applications you will be working with include the Block Storage, Compute, and Object Storage applications: The *Block Storage* application enables the attachment of block volumes to instances and the management of block volumes and volume snapshots. The *Compute* application enables the management of instances and their

related configuration, such as security groups and key pairs. The *Object Storage* application enables objects to be uploaded, viewed, and downloaded from the Object Storage service. Uploads are limited in size to 10MB.

1.2.2 Download API Access Credentials

API Access credentials are provided to enable users and administrators to interact with OpenStack and EC2 compatible programmable interfaces.

1. Open the user menu by clicking the *user* icon near the top right of the Home page, and then select *API Access*.
2. Select the project for which you wish to download the credentials, then click *Download.*

See Also:

Advanced Interaction with CLIs and APIs

1.2.3 Log Out

You can log out from the Home page or any internal application by opening the user menu and clicking *Sign Out*.

1.3 Create or Launch Instances

An *instance* is the basic compute resource provided by the Nebula One system. An instance is a virtual machine whose virtual hardware is defined by its flavor and whose initial software contents are defined by its image.

1.3.1 Launch an Instance (Basic)

By default, the basic form for launching instances will be shown at the top of the page. The basic form will launch instances using only the default security group and key pair. To specify alternate security groups or key pairs see Launch an Instance (Advanced).

1. From the home page click the *Compute* application.
2. In the Compute application, navigate to the *Instances* page.
3. If the Advanced form is shown, click the *Basic* button in the lower left of the form.
4. Select an *image* or snapshot in the Basic form by clicking on the appropriate icon. An image is a prefabricated Operating System archive that defines the initial state of an instance.
5. Provide a name for the instance.
6. Choose the flavor of the instance (based on a virtual hardware template) using the size slider. The size selector displays the amount of *quota* that will be consumed by launching the instance, where blue numbers represent virtual hardware characteristics for the chosen flavor and bar graphs show quota usage before the instance is launched (dark grey), and additional usage after the instance is launched (blue).
7. Click *Launch*.

The progress of the launch is displayed. If this was your first instance, then the NebulaLaunchKey was created for you. You should click the *Download* button to save this key to your personal computer to access your instances. Subsequently launched images will use the existing NebulaLaunchKey.

Once launch progress has completed, the instance is ready for use and will show as Active in the Instance list.

1.3.2 Launch an Instance (Advanced)

The advanced form allows you to select which key pair and security groups an instance will use.

1. In the Compute application, navigate to the *Instances* page.
2. If the basic form is shown, click the *Advanced* button in the lower left of the form.
3. Choose the image or snapshot from the drop down list. An image is a prefabricated Operating System archive that defines the initial state of an instance; a snapshot is a disk image from a running instance. It stores everything from the *Root Disk*. Typically, image and snapshot names describe the OS and/or configuration contained within, though user-created images and snapshots might not adhere to this model.
4. Create a name for the instance.
5. Choose a *key pair*, if necessary. In some cases, an SSH key pair might not be needed to access the instance.
6. Choose one or more security groups.
7. Using the size slider, choose the flavor of the instance based on a virtual hardware template. The size selector displays the amount of quota that will be consumed by launching the instance, where blue numbers represent virtual hardware characteristics for the chosen flavor and bar graphs show quota usage before this instance is launched (dark grey) and additional usage after this instance is launched (blue).
8. Click *Launch.*

The progress of the launch is displayed. If the NebulaLaunchKey was created, it will be available for download in the Instance Details area. Once launch progress has completed, the instance is ready for use and will show as Active in the instance list.

1.4 Access an Instance from the Virtual Console

The Nebula One system provides *virtual console* access to every instance. While instances are normally accessed through the network, the virtual console can be useful to check the availability of an instance and to review the boot and halt messages when debugging.

1. From the Home page click the *Compute* application.
2. In the Compute application, navigate to the Instances page.
3. Click the name of an instance to navigate to that instance's detail page.
4. Click the *Console* tab to display the instance console.

1.5 Access an Instance Over the Network

The Nebula One system automatically assigns a unique *Fixed IP* address for each instance. This IP address can be either accessible or non-accessible from outside the Nebula One system depending on the system's configuration. If accessible, a Private IP is all that is required to access the instance. If non-accessible, a floating IP address must be assigned to the instance in order to access the instance from outside the cloud. Ask your Cloud Administrator how your Nebula one is configured.

See Also:

ip-configuration

Security groups control all inbound network access to an instance according to their inbound firewall rules. By default, all traffic is blocked. If an instance should be accessible through a private or floating IP but connections to the instance are failing, access might be blocked by the absence of a security group rule permitting access.

1.6 Terminate (Delete) an Instance

Terminating an instance ends its existence immediately. All root disk and ephemeral disk data is no longer accessible. Attached block volumes are detached with their data intact.

1. In the Compute application, navigate to the *Instances* page.
2. Choose *Terminate* from the Action Menu of the target instance.
3. Choose *Confirm*.

1.7 Create an Instance Snapshot

An *instance snapshot* captures the contents of an instance at the time of the snapshot. Snapshots can be used to launch new instances; these new instances will have initial contents identical to the state of the snapshot's source instance at the time the snapshot was taken. Snapshots are not dependent upon their source instances and might be used even if the source instance has been deleted.

1. In the Compute application, navigate to the *Instances* page.
2. Choose *Snapshot* from the *Actions Menu* of the target instance.
3. In the dialog, create a name for the snapshot and click *Create*. Note that creating a snapshot interrupts the running instance.

The task status for the instance will update to show that a snapshot is being created. Check the new instance snapshot on the *Images and Snapshots* page.

1.8 Launch an Instance from a Snapshot

Once a snapshot has been created, it can be used in place of an image to launch a new instance. To launch an instance from a snapshot, select the snapshot you wish to use from the list of images.

Once created, an instance launched from a snapshot is identical to an instance launched from an image; you can then configure the new instance as needed.

1.9 Delete an Instance Snapshot

Instance snapshots can be deleted at any time without affecting running instances.

1. In the Compute application, navigate to the *Images & Snapshots* page.
2. Choose *Delete* from the Action Menu of the target instance snapshot.

1.10 Manage Security Groups

A security group defines a set of firewall rules for allowing inbound access to an instance. These rules can only permit access, as all inbound access to an instance is blocked by default.

One or more security groups can be associated with an instance. It is helpful to create several security groups defining rules for specific applications rather than a single security group containing all the rules for a single instance. This

approach provides the flexibility to address the specific needs of each instance without creating a unique security group for each instance.

Security groups are specified when an instance is created (launched). While security groups cannot be added to or removed from an instance that has already been created, the rules for those security groups can still be modified. These changes will apply immediately to any instances using that security group.

A default security group is included in each project. While this group cannot be deleted, its rules can be modified. All instances launched with the basic form use only this security group. If no security group is specified in the Nebula One command line interface when an instance is launched, the default security group is associated with that instance automatically.

If you need network access to an instance, its associated security groups must have rules that allow access through required ports; for example, port 22 for SSH access or port 3389 for RDP access. These rules can be defined in any security group assigned to the instance.

1.10.1 Create a Security Group

1. In the Compute application, navigate to the *Security Groups*.
2. Assign a name and description to the security group.
3. Click *Create.*

The new security group appears in the Security Groups list.

Note: Security groups are created without rules; rules can be added by editing the security group.

1.10.2 Manage Security Group Rules

Rules can be added to or removed from a security group at any time. Changes will apply to any instances using that security group. This behavior applies to the default security group as well.

Add Rules to a Security Group

1. In the Compute application, navigate to the *Security Groups* page.
2. Choose *Edit* from the Actions Menu of the target security group.
3. Enter the *protocol, port range start*, *port range stop*, and *source CIDR* or *source security group*.
4. In the *Protocol* menu, specify the TCP, UDP, or ICMP protocol. The Port Range Start and End define different values depending on the currently selected protocol. For TCP and UDP rules, these fields define the range of server-side ports for the rule. A single port can be specified by using the same value for both fields. For ICMP rules, the Port Range Start field defines the ICMP type while the Port Range End field defines the ICMP code. Either of these ICMP fields will accept the value -1 as a wildcard for all ICMP types. The Source CIDR field defines the client IP addresses to which the rule applies. To specify all client IP's, use 0.0.0.0/0.
5. Click *Create.*

The new rule appears in the security group rules list.

Remove Rules from a Security Group

Rules can be removed from a security group at any time. Changes will apply to any instances using that security group. This behavior applies to the default security group as well.

1. In the Compute application, navigate to the *Security Groups* page.
2. Choose *Edit* from the Actions Menu of the target security group.
3. Click *Delete* for the target security group rule.

View Security Groups for an Instance

If you do not have the expected network access to an instance, the instance details page provides a security group overview that serves as an excellent debugging tool. This page displays all security groups assigned to an instance and all rules belonging to those security groups.

1. In the Compute application, navigate to the *Instances* page.
2. Click the name of the target instance.

All security groups and security group rules are shown in the security group overview.

1.11 Manage Floating IP Addresses

Floating IPs are allocated from a global pool created by the administrator, from which a project can reserve a number of addresses. The maximum number of floating IP addresses that may be allocated to a project is determined by that project's quota.

If private IP addresses are not accessible outside of the Nebula One system, assigning a floating IP to an instance will allow external access to that instance. Each floating IP can only be assigned to a single instance. An instance can have more than one floating IP assigned to it.

1.11.1 Allocate Floating IP Addresses to a Project

1. In the Compute application, navigate to the *Floating IPs* page.
2. Click *Allocate New Floating IP*.

The new IP address will be added to the floating IP address list.

1.11.2 Assign a Single Floating IP Address

Use this method to quickly assign a floating IP to an instance with no floating IP addresses.

1. In the Compute application, navigate to the *Instances* page.
2. Click the *Add* button in the Floating IP column for the target instance.
3. Choose a floating IP in the IP Address drop down menu.
4. Click *Add*.

The selected floating IP replaces the *Add* button. Additional IP addresses can be assigned from the Floating IPs page.

1.11.3 Assign One or More Floating IPs Addresses

Use this method to add one or more floating IPs to an instance.

1. In the Compute application, navigate to the *Floating IPs* page.
2. Choose *Add to Instance* from the Actions Menu of the target floating IP.
3. Select the instance from the Instance drop down.
4. Click *Add.*

The Instances page lists all assigned floating IPs.

1.12 Manage Key Pairs

A Key Pair provides SSH access for an instance without using a password. Each key pair consists of a public key and a private key and can be generated by the Nebula One System or by an external key pair generator. In either case, the public key is managed by the Nebula One System and is associated with instances, while the private key is held by a user and never shared. Once an instance has launched its associated key pair cannot be changed.

1.12.1 Download the NebulaLaunchKey Key Pair

The NebulaLaunchKey key pair is used for all instances launched with the basic instance launch method and any instance launched with the advanced form for which NebulaLaunchKey is specified in the key pair field. This key pair is automatically generated the first time it is invoked and will be available for download in the Instance Details area.

Warning: This key pair cannot be downloaded in the future as this would compromise the security of that key pair. If you no longer have access to the private key of the NebulaLaunchKey key pair see Import a Key Pair and Launch an Instance (Advanced).

1.12.2 Import a Key Pair

A key generation program (for example, **ssh-keygen** on a Linux/Unix system) can be used to create a key pair outside of the Nebula One System. In order to import a key pair, you must provide the public key.

1. In the Compute application, navigate to the *Key Pairs* page.
2. Provide the name for the key pair, and copy and paste the public key into the Public Key field.
3. Click *Import.*

The new key pair will be shown in the Key Pair list.

1.12.3 Specify the key pair to be associated with an instance

1. In the Compute application, navigate to the Instances page.
2. Display the advanced form if the basic form is displayed.
3. Specify the appropriate key pair.

To access an instance configured with a key pair, the private key must be specified in the client application. This private key will be related to a user, for example:

```
# ssh –l user-to-login-as –i ~/path/to/key.pem instance-ip
```

See Also:

ip-configuration

1.13 Manage Volumes

The Nebula One System enables the creation of virtual block devices, known as block volumes. These block volumes persist independently from instances: any data created or modified on the volume by an instance will remain even if that instance is deleted. Each block volume can be moved from instance to instance but can only be attached to one instance at a time. Note that volumes need to be partitioned and formatted in an OS-specific manner.

1.13.1 Create a New Volume

1. In the Block Storage application, navigate to the *Block Volumes* page.
2. Specify a name, description, and a size (in gigabytes).
3. Click *Create.*

The new block volume will be shown in the block volumes list.

1.13.2 Attach a Single Volume to an Instance

This method allows a single volume to be quickly attached to an instance but cannot attach further volumes to that instance.

1. In the Compute application, navigate to the *Instances* page.
2. Click the *Attach* button in the Volumes column for the target instance.
3. Select a volume.
4. Click *Attach.*

The selected volume replaces the Attach button in the instances list. To attach further volumes, see Attach One or More Volumes to an Instance.

1.13.3 Attach One or More Volumes to an Instance

This method allows the attachment of volumes to instances that already have volumes attached.

1. In the Block Storage application, navigate to the *Block Volumes* page.
2. Choose *Attach* from the Actions Menu of the target volume.
3. Select an instance.
4. Click *Attach.*

The Instances page lists all attached volumes.

1.13.4 Detach a Volume from an Instance

Detaching a volume from an instance enables that volume to be attached to a different instance. Before detaching a volume from an instance, make sure that the volume is quiesced (that is, unmounted as a file system or database volume) inside the instance. Detaching an active volume might risk data corruption within that volume.

1. In the Block Storage application, navigate to the Block Volumes page.
2. Choose Detach from the Action Menu of the target volume.

Wait until the Status for the target volume has returned to Available before acting upon it further.

1.13.5 Delete a Volume

1. In the Block Storage application, navigate to the *Block Volumes* page.
2. Choose *Delete* from the Action Menu of the target volume.

1.13.6 Create a Volume Snapshot

A volume snapshot captures the contents of a volume at the time of the snapshot. Volume snapshots can be used to initialize new volumes; these new volumes will have initial contents identical to the state of the snapshot's source volume at the time the snapshot was taken. Volume snapshots are not dependent on their source volumes and might be used even if the source volume has been deleted.

Volume snapshots can only be created from volumes not attached to instances. Be sure to detach the volume if it is attached to an instance.

1. In the Block Storage application, navigate to the *Block Volumes* page.
2. Choose *Snapshot* from the Action Menu of the target volume.
3. Provide the name and description for the new snapshot.
4. Click *Create*.

The new volume snapshot will be shown in the storage snapshots list.

1.13.7 Create a Volume from a Volume Snapshot

1. In the Block Storage application, navigate to the *Snapshots* page.
2. Choose *Create Volume* from the Action Menu of the target storage snapshot.
3. Provide the name, description, and size (in gigabytes) for the new volume. The size defined for this new volume may be larger, but not smaller, than the source volume.
4. Click *Create.*

The new volume is shown in the block volumes list.

1.13.8 Delete a Volume Snapshot

1. In the Block Storage application, navigate to the *Snapshots* page.
2. Choose *Delete* from the Action Menu of the target storage snapshot.

1.14 Manage Instances

1.14.1 Pause or Suspend an Instance

Pausing an instance effectively freezes its virtual CPU. The amount of memory consumed by this instance remains constant. *Suspending* an instance freezes an instance and writes its running state to disk. The memory consumed by this instance is freed.

To pause or suspend an instance:

1. In the Compute application, navigate to the *Instances* page.
2. Choose *Pause* or *Suspend* from the Action Menu of the target instance.

1.14.2 Unpause or Resume an Instance

Unpausing an instance reverses the pausing of an instance and replaces the *Pause* action in the Action Menu. *Resuming* an instance reverses the suspending of an instance and replaces the *Suspend* action in the Action Menu.

1.15 Advanced Interaction with CLIs and APIs

APIs are a powerful way to manage your system programatically. Nebula One implements both OpenStack and EC2 APIs for many resources.

First, download your API access credentials. See *Download API Access Credentials*. There are varying *command line clients* for interacting with the OpenStack APIs. Consult the OpenStack documentation to learn more about direct API access.

1.15.1 More Resources and Tools

- Cloudenvy - CloudEnvy allows developers to easily spin up instances for development in an OpenStack cloud.
- Knife OpenStack - A Chef knife plugin for interacting with OpenStack
- Puppet - OpenStack with Puppet
- Salt Cloud Salt is a configuration management system. Salt Cloud allows you to manage OpenStack (and other) clouds.

1.16 Glossary

API Application Programming Interface. Nebula One implements both OpenStack and AWS APIs in many cases. For more information refer to *Advanced Interaction with CLIs and APIs*.

Block Storage Block Storage services provide the ability to attach, detach, and snapshot volumes to instances, allowing you to move data between instances and keep data available on a block (drive-like) device without any attached instance running.

Cinder OpenStack refers to its block storage service internally as Cinder.

Compute A generic term to indicate virtual server resources consisting of RAM, Virtual CPU units, a root disk and an ephemeral disk.

Fixed IP A fixed IP address is automatically assigned by the compute service.

Flavor A flavor is a definition, or template, for the resources that an instance will consume.

Floating IP A Floating IP address is a mechanism for associating a given IP address with an instance. It is typically used in scenarios where a service always responds to a given address, but the instance behind it can be swapped. In some configurations, a floating IP address is required to access an *instance* from outside the Nebula One system.

Glance OpenStack refers to its image service internally as Keystone.

Image An image is the base that an instance boots from. It is typically a base operating system configured for use with your Nebula One system. Properly configured images will typically install the specified *key pair* at boot.

Instance An instance is a virtual machine running on a compute node. It belongs to a *project*, and its size parameters are controlled by a *flavor*.

Instance Snapshot An instance snapshot is used to create a disk image from a running instance. It stores everything from the *Root Disk*. New instances can be created from a snapshot.

Key Pair A key pair uses asymmetric key algorithms to publish a private key that instances and the cloud can use to validate access to an instance. You, as a user have both a public and a private key.

Keystone OpenStack refers to its authentication service internally as Keystone.

Nebula Cloud Edge Nebula Cloud Edge is a network device that connects multiple controllers together to present the Nebula One as a contiguous system to the rest of your network.

Nova OpenStack refers to its compute service internally as Nova.

Object Storage Object storage refers to the service for generic blob storage. Nebula One implements the Swift API.

Private IP Private IP refers to a *Fixed IP* in configurations where the internal network and the external network are segregated. For more information see *ip-configuration*.

Project A project is a container used to manage resource allotments. For more information see *projects*. OpenStack uses tenant and project interchangeably.

Public IP Public IP refers to a *Floating IP* in configurations where the internal network and the external network are segregated. For more information see *ip-configuration*.

Quota A quota is assigned to a project to set resource allotments. Quotas are representative of the resources a user is allowed to use, and quota indicators do not necessarily represent that resources requested are available in your system.

Root Disk The root disk for an instance typically contains the entire operating system. It is kept intact if the image is snapshotted. It is always physically located on the same compute node as the instance that is used.

Security Group A security group manages ingress to an instance.

Swift OpenStack refers to its object storage service internally as Swift.

Virtual Console The virtual console is accessible through the UI to provide access to instances when network access is undesirable or inaccessible.

Volume A volume is an external disk resource to an instance. It is an iSCSI-attached disk that can be attached or detached at will and that survives instance termination.

Volume Snapshot A volume snapshot is used to create a disk image from an existing *Block Storage* volume. Volume Snapshots can not be attached to instances.